JOHN M. NEUKOM (SBN 275887)
JAMES Y. PAK (SBN 304563)
SKADDEN, ARPS,
SLATE, MEAGHER & FLOM LLP
525 University Avenue
Palo Alto, California 94301-1908
Telephone: (650) 470-4500
Facsimile: (650) 470-4570
john.neukom@skadden.com
james.pak@skadden.com

DOUGLAS R. NEMEC (*pro hac vice*)
RACHEL R. BLITZER (*pro hac vice*)
LESLIE A. DEMERS (*pro hac vice*)
ANTHONY P. BIONDO (*pro hac vice*)
SKADDEN, ARPS,
SLATE, MEAGHER & FLOM LLP
One Manhattan West
New York, New York 10001
Telephone: (212) 735-3000
Facsimile: (212) 735-2000
douglas.nemec@skadden.com
rachel.blitzer@skadden.com
leslie.demers@skadden.com
anthony.biondo@skadden.com

Attorneys for Plaintiff,
FORTINET, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

FORTINET, INC.,

Plaintiff,

v.

FORESCOUT TECHNOLOGIES, INC.,

Defendant.

Case No. 3:20-cv-03343-EMC

PLAINTIFF FORTINET, INC.'S NOTICE OF MOTION AND MOTION TO DISMISS COUNTERCLAIMS PURSUANT TO FED. R. CIV. P. 12(b)(6)

DATE: September 23, 2021
TIME: 1:30 p.m.
LOCATION: Courtroom 5, 17th Floor

Hon. Edward M. Chen

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

OTHER AUTHORITIES

NOTICE OF MOTION AND MOTION

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that Plaintiff Fortinet, Inc. ("Fortinet") hereby moves to dismiss Counts I, VIII, IX, XI and XII asserted in Defendant Forescout, Inc.'s ("Forescout") Answer and Counterclaim, Dkt. No. 107, and will present its motion on September 23, 2021, at 1:30 p.m., or as soon thereafter as the matter may be heard, in Courtroom 5, 17th Floor, of the U.S. District Court for the Northern District of California, located at 450 Golden Gate Ave., San Francisco, California, 94102.

Fortinet requests that these Counterclaims be dismissed with prejudice, pursuant to Rule 12(b)(6), as Forescout fails to state a claim upon which relief can be granted for several reasons. First, the claims of the patents asserted in Counts VIII, IX, XI, and XII are invalid under 35 U.S.C. § 101 as they are directed to an abstract idea and lack any inventive concept. *See Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208 (2014). Second, the action for tortious interference brought in Count I is not tenable for three independently dispositive reasons: (1) the alleged statements are protected by federal law which preempts the state law claim, (2) the alleged conduct is not subject to this Court's subject matter jurisdiction, and (3) the alleged conduct does not satisfy California law to state a claim for tortious interference.

STATEMENT OF ISSUES TO BE DECIDED

(1) Whether the claims of the patents asserted in Counts VIII, IX, XI, and XII of Forescout's counterclaims are patent-ineligible under 35 U.S.C. § 101;

(2) Whether the state law claim (Count I) is preempted under the federal Patent Act;

(3) Whether the state law claim (Count I) is subject to the Court's subject matter jurisdiction;

(4) Whether the state law claim (Count I) is actionable under California law.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Forescout has brought several counterclaims against Fortinet, including asserting infringement of six patents as well as a claim for tortious interference based on supposed extrajudicial statements made by Fortinet following the commencement of this lawsuit. *See* Dkt. 107 ("Ans.") ¶¶

148-213. Fortinet hereby challenges the subject matter eligibility of four of those patents,[1] and moves to dismiss the tortious interference claim on multiple grounds.

The Court should dismiss the patent infringement claims of Counts VIII, IX, XI, and XII under 35 U.S.C § 101, since the claims of those patents are directed to non-patentable abstract ideas and do not recite additional elements sufficient to transform them into patentable material. Forescout's patents claim bare abstract ideas in the field of network security rather than concrete inventions, and either call for those ideas to be implemented on generic computer hardware used in a conventional way, or in some claims simply recite the idea itself with nothing more.

The tortious interference claim fails for multiple reasons. To begin, a party's communications about its non-sham patent infringement allegations are protected by federal law and preempted from adjudication here. Further, this Court lacks subject matter jurisdiction over any portion of Count I that is not preempted, as the remaining claim does not fall within the supplemental jurisdiction of 28 U.S.C. § 1367, and in any event does not plead a plausible claim of tortious interference under California law, as Forescout has not alleged facts giving rise to an independently actionable wrongful act or a specific business relation that was interfered with.

II. LEGAL STANDARDS

1. Rule 12(b)(6) – Motion to Dismiss

Rule 12(b)(6) permits a party to raise by motion the defense that the complaint "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). Specifically, a complaint must include a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a). However, the allegation of "facts that are 'merely consistent with' a defendant's liability" fall short of presenting a plausible entitlement to relief. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)). Similarly, courts need not accept as true "legal conclusions" contained in the complaint. *Id.* at 678-79 (citing *Twombly*, 550 U.S. at 555).

[1] Fortinet is not challenging the subject matter eligibility of the patents asserted in Counts VII and X at this time, but reserves the right to do so at a later date.

In light of the Supreme Court's admonition that patent eligibility is a "threshold" issue, *Bilski v. Kappos*, 561 U.S. 593, 602 (2010), the Federal Circuit has repeatedly confirmed that disposing of patent-ineligible claims on a motion to dismiss is appropriate, as no claim for relief can be based on unpatentable subject matter. *See, e.g., Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 717 (Fed. Cir. 2014); *buySAFE, Inc. v. Google, Inc*., 765 F.3d 1350, 1351-52 (Fed. Cir. 2014). When considering a Section 101 motion to dismiss, "a court need not 'accept as true allegations that contradict matters properly subject to judicial notice or by exhibit,' such as the claims and the patent specification." *Secured Mail Sols. LLC v. Universal Wilde, Inc.*, 873 F.3d 905, 913 (Fed. Cir. 2017) (citation omitted).

2. 35 U.S.C. § 101 – Patentable Subject Matter

Section 101 of the Patent Act defines patentable subject matter as "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. It has long been held that patents cannot claim abstract ideas, laws of nature, or natural phenomena. *Mayo Collaborative Servs. v. Prometheus Lab'ys, Inc.*, 566 U.S. 66, 70 (2012). Courts apply a two-step test for determining whether claims are directed to patent-ineligible subject matter. *Alice Corp.*, 573 U.S. at 217-18. First, the court must "determine whether the claims at issue are directed to a patent-ineligible concept," such as an abstract idea. *Id.* at 218. Second, if the claims are directed to an abstract idea, the court must then "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Id.* at 217 (quoting *Mayo*, 566 U.S. at 78, 79).

At step one, when evaluating whether the claims are "directed to" a patent-ineligible concept, such as an abstract idea, the court engages in a process described as "looking at the 'focus' of the claims." *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016). The analysis looks to the claim's "character as a whole" and does not require "evaluating each claim limitation in a vacuum," but where a "bare abstract idea" is "at the core" of a claim, courts have found claims to be directed to patent-ineligible subject matter. *Ericsson Inc. v. TCL Commuc'n Tech. Holdings Ltd.*, 955 F.3d 1317, 1326 (Fed. Cir. 2020) (citing *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335

(Fed. Cir. 2016)). A claim does not pass step one when it merely recites "a generic environment in which to carry out the abstract idea," comprised of "conventional components [that] perform only their basic functions" and "set forth at a high degree of generality." *Yu v. Apple, Inc.*, 1 F.4th 1040, 1043-44 (Fed. Cir. 2021).

As to step two, a court must evaluate whether the claims recite additional elements sufficient to "transform the nature of the claim" into a patent-eligible application. *Alice Corp.* 573 U.S. at 217 (quoting *Mayo*, 566 U.S. at 78, 79). In doing so, courts will "consider the elements of each claim both individually and 'as an ordered combination.'" *Id.* While the analysis here is "aided by a consideration of the specification," one cannot "import details from the specification if those details are not claimed." *Ericsson*, 955 F.3d at 1328 (citing *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 769 (Fed. Cir. 2019)). Where a "claimed configuration does not add sufficient substance to the underlying abstract idea" and merely serves as "a conduit for the abstract idea," the claim is missing an inventive concept, "even if [the claim] recites novel subject matter." *Yu*, 1 F.4th at 1045 (citing *In re TLI Commc'ns. LLC Pat. Litig.*, 823 F.3d 607, 612 (Fed. Cir. 2016); *SAP Am. Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1163 (Fed. Cir. 2018)).

Whether a claim is patent ineligible is a question of law. *Accenture Glob. Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1340-41 (Fed. Cir. 2013). Courts routinely dismiss patent-ineligible claims at the pleading stage. *See, e.g., Ultramercial, Inc., v. Hulu,* LLC, 772 F.3d 709, 717 (Fed. Cir. 2014); and *Voip-Pal.Com, Inc. v. Apple Inc.*, 375 F. Supp. 3d 1110 (N.D. Cal. 2019, *aff'd sub nom., Voip-Pal.com, Inc. v. Twitter, Inc.*, 798 F. App'x 644 (Fed. Cir. 2020)); *PersonalWeb Techs. LLC, v. Google, LLC,* Nos. 2020-1543, 2020-1553, 2020-1554, 2021 WL 3556889, at *7 (Fed. Cir. Aug. 12, 2021). Dismissal is appropriate "[w]hen there is no genuine issue of material fact" as to the invalidity of the patents. *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018). Moreover, "if the patentee does not present any meaningful argument for the distinctive significance of any claim," a court may consider a claim representative. *Id.* at 1365. Where a representative claim exists, "[a]ddressing each of the asserted claims is unnecessary when 'all the claims are substantially similar and linked to the same abstract idea.'" *Intell. Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1316 n.9 (Fed. Cir. 2016).

3. California Law – Tortious Interference with Business Relationships

In California, intentional interference with prospective economic advantage has five elements: (1) the existence, between the plaintiff and some third party, of an economic relationship that contains the probability of future economic benefit to the plaintiff; (2) the defendant's knowledge of the relationship; (3) intentionally wrongful acts designed to disrupt the relationship; (4) actual disruption of the relationship; and (5) economic harm proximately caused by the defendant's action. *Roy Allan Slurry Seal, Inc. v. Am. Asphalt S., Inc.*, 2 Cal. 5th 505, 512 (2017). The defendant's intentional acts must be wrongful and independently actionable by some measure beyond the fact of the interference itself. *Della Penna v. Toyota Motor Sales, U.S.A., Inc.*, 11 Cal. 4th 376, 393 (1995). The tort does not punish lawful competition, choice of commercial relationships, or pursuit of commercial objectives even if carried out with an improper motive. *Korea Supply Co. v. Lockheed Martin Corp*., 29 Cal. 4th 1134, 1158-59 (2003).

4. Federal Law – Preemption of State Tort Claims Based on Communications Asserting Federal Patent Rights

Federal patent law preempts state law tort liability for a patentholder's good faith conduct in communications asserting infringement of its patent and warning about potential litigation. *Globetrotter Software v. Elan Comput. Grp., Inc*., 362 F. 3d 1367, 1374 (Fed. Cir. 2004). Courts apply Federal Circuit law in deciding whether the patent laws preempt a state law tort claim in a patent case. *Id.* at 1374. The Federal Circuit has held that extrajudicial statements, such as good faith communications about the applicability of patent rights, are protected against state law tort claims. *Id.* at 1376-77. It has also held that this protection is not narrowly limited to pre-litigation statements, and has held, for example, that federal law also preempts state law that punishes "publicizing a patent in the marketplace" in the absence of bad faith. *Id.* at 1377, n.9 (quoting *Hunter Douglas, Inc. v. Harmonic Design, Inc.*, 153 F.3d 1318, 1336 (Fed. Cir. 1998)). Additionally, it has held that preemption applies to communications made "whether by direct notice to [the] potential infringers or by publicity release." *Mikohn Gaming Corp. v. Acres Gaming, Inc.*, 165 F.3d 891, 897-98 (Fed. Cir. 1998).

5. Federal Law – Subject Mater Jurisdiction – Supplemental Jurisdiction

Under 28 U.S.C. § 1367, a federal district court may hear state law claims "that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution." It may decline to hear such a claim if "a novel or complex issue of State law," "substantially predominates" over the federal claims, if it has dismissed the federal claims, or in exceptional circumstances with other compelling reasons. 28 U.S.C. § 1367(a). In order for a claim to "form part of the same case or controversy," *id.*, the claims must "derive from a common nucleus of operative fact." *United Mine Workers of Am. v. Gibbs*, 383 U.S. 715, 725 (1966).

III. ARGUMENT

1. Forescout's Asserted Patents are Invalid Under 35 U.S.C. § 101

Each of the four patents addressed herein is directed to a bare abstract idea, implemented on generic hardware, performing generic tasks, and arranged in an overall conventional way. While the patents each have distinct claims, their claims are not dissimilar to those the Federal Circuit invalidated in *Ericsson*, which were held to be directed to the abstract idea of controlling access to, or limiting permission to, resources. 955 F.3d at 1326. And while several of the claims are written in "technical jargon," as in *Ericsson*, this alone does not save them, as a "close[r] analysis" of the claims reveals that they require nothing more than the respective abstract idea which lies at the "core" of each claim. *Id.* Indeed, the claims add little if anything to the abstract ideas they recite, apart from the basic context of a conventional computer network, and the use of conventional components performing their basic functions to implement those ideas. *See Yu*, 1 F.4th at 1043-44.

a. U.S. Patent No. 6,363,489 (the '489 Patent)

The '489 Patent is related to a method for automatic intrusion detection and intruder diversion in a network. It claims, in short, a method of providing marked false data to a suspected intruder, and then waiting for someone to show up presenting that marked data—not unlike providing a bank robber with marked bills, and waiting for them or their co-conspirators to try and spend the money. The application from which the '489 Patent issued was filed on Nov. 29, 1999, which means it expired on Nov. 29, 2019. According to its specification, the claimed invention of the '489 Patent is meant to assist in "detecting the stage in which information is gathered" by unauthorized users on a network, identifying those users when they attempt to gain access, and then preferably blocking them from such attempts. '489 Patent at 1:53-59. Claim 1 of the patent recites a method involving providing false data, dubbed an "earmark," to suspected unauthorized information gatherers, monitoring subsequent communications for that earmark, and then applying intrusion handling procedures to these communications. *Id.* at Claim 1. In other words, it claims the simple ruse of baiting intruders with false information and then flagging when they attempt to use that information. The dependent claims add little, reciting, *e.g.*, communicating via units of data called packets (Claim 2), using a "mark destination address" (*i.e.*, a fake destination on the network, reserved to lure in intruders) to detect information gathering (Claims 3, 4), alerting the system administrator to intruders (Claim 5), dropping communications of intruders (Claim 6), redirecting intruder communications to a "secure zone" (Claims 7, 8), reciting a handful of common information gathering procedures that suspicious users may employ, including a "scan" to search for vulnerable services on the network (Claim 9), using a means of detecting a scan by "determining a profile of ranges of legitimate packet behavior" and monitoring for deviation from that behavior (Claim 10, 11), imitating a "non-existent service" as a mark (Claims 12-14), and system claims.

Accordingly, the '489 Patent is directed to the abstract idea of detecting unauthorized users by baiting them with false information. Its claims include technical terms, but otherwise describe a method and system with its implementation left to the discretion of the reader. The first independent claim of the '489 Patent is representative, and recites:

> *1. A method for detecting and handling a communication from an unauthorized source on a network, the method comprising the steps of:*
>
> *(a) receiving the communication from the unauthorized source;*
>
> *(b) analyzing the communication for detecting an information gathering procedure;*
>
> *(c) if said information-gathering procedure is detected, indicating a source address of the communication as a suspected network reconnaissance collector;*
>
> *(d) returning an earmark to said suspected reconnaissance collector, such that said earmark includes specially crafted false data, and such that said earmark includes data that can serve to identify an unauthorized source;*
>
> *(e) analyzing each subsequent communication for a presence of said earmark;*

> *(f) if said earmark is present, indicating source address of the communication as a suspected network reconnaissance collector, and*
>
> *(g) if said source address is said intruder source address, applying intrusion handling procedures towards the communication from said intruder source address.*

'489 Patent at Claim 1. As explained below, this claim recites nothing more than an abstract idea, and an instruction to the reader to apply that idea in the context of a computer network. Further, it adds nothing more to this idea beyond a bare recitation of the idea itself. Accordingly, the '489 Patent is invalid.

i. The '489 Patent's Claims are Directed to an Abstract Idea

The '489 Patent is directed to the abstract idea of detecting unauthorized users by baiting them with false information. As the applicant described it during prosecution, the claimed invention revolves around sending "bait" consisting of "falsified data" to an intruder, and then waiting for that falsified data to appear to take action against them. *See* '489 Patent File History, Response to Office Action of March 27, 2001, Remarks (Ex. B) at 1-2.[2] Thus, its claims may be summarized as requiring that a conventional machine on a conventional network receive communications, detect information gathering procedures in those communications through some unspecified method, send an earmark to those information gatherers, and then analyze subsequent communications for the presence of that earmark, all while keeping track of the source address of the parties involved. It's a classic ruse, where the machine sends false but earmarked information to suspected bad actors, and then waits to see who turns up presenting that earmarked data.

Like the idea of an intermediated settlement in *Alice*, the idea of "baiting" an intruder with false information is a simple and well-known "method of organizing human activity," which is applied here by computers in the context of network security. 573 U.S. at 220. Indeed, this particular method of organizing an activity has been applied by humans historically, as in the example of bank robbers and marked bills. In other fields, for example, map makers would add "false facts" like fake streets to their maps (*i.e.*, in the language of the claims here, an earmark including specially crafted

[2] To the extent Fortinet relies upon the file histories of the '489 and '116 Patents in this motion, it requests that the Court take judicial notice of Forescout's representations to the patent office during prosecution. *See, e.g., see Coffelt v. NVIDIA Corp.*, No. CV16-0045 SJO (KKX), 2016 WL 7507763, at *2 n.3 (C.D. Cal. June 21, 2016), *aff'd*, 680 F. App'x 1010 (Fed. Cir. 2017) (taking judicial notice of the entire prosecution history of a patent).

false data), and then monitor the maps produced by their competitors (*i.e.*, monitoring subsequent communications) to determine the identity (*i.e.*, the source address) of those parties copying from them (*i.e.*, gathering information), to then sue them (*i.e.*, apply intrusion handling procedures). *See, e.g.*, *Nester's Map & Guide Corp. v. Hagstrom Map Co.*, 796 F. Supp. 729 (E.D.N.Y. 1992) (copyright lawsuit after the copying of false streets from a map). Apart from the limited use of technical jargon and the automation of its implementation by a computer, the principle is the same. The claims here seek to monopolize on one of the oldest forms of deception as applied to computer networking.

As the Federal Circuit has observed, a "wide variety of well-known and other activities constitute abstract ideas." *Ericsson*, 955 F.3d at 1327. The abstract idea to which the claims in the '489 patent are directed is not dissimilar from that found in *Ericsson*. There, the court considered claims which it found to be directed to the abstract idea of controlling access to, or limiting permission to, resources. *Id.* at 1326. The claims there included several elements that purported to flesh out the claims, reciting a claim including, *inter alia*, a platform, an abstract controller, an interception module, a decision entry, application domain software, and a software services component. *Id.* at 1325-26. However, the court looked past this "technical jargon" to instead focus on the claim's "character as a whole," finding that the claims were directed to an abstract idea. *Id.* at 1326-27 (citing *Enfish*, 822 F.3d at 1335). Moreover, the Federal Circuit found that the idea of the claims in *Ericsson* was an abstract "method of organizing human activity" by comparison to existing human activities – such as "loaning materials only to card-holding members," "allowing certain employees entrance to only certain floors," or "offering or denying loans to applicants based on suitability and intended use." *Id.* at 1327. Here too, the act of baiting an intruder with false information is a well-known human activity, not dissimilar from the marked bills and false map entries discussed above.

Likewise, the Federal Circuit recently found claims of an asserted patent to be directed to the abstract idea of "collecting and analyzing information for financial transaction fraud or error detection." *Bozeman Fin. LLC v. Fed. Rsrv. Bank of Atlanta*, 955 F.3d 971, 977 (Fed. Cir. 2020), *cert. denied*, 141 S. Ct. 1053 (2021). In *Bozeman*, the invention was directed to a method of preventing check fraud by "receiving financial transaction data from two sources including the point of sale and comparing that data to verify a transaction," not dissimilar from the '489 Patent's claimed method of preventing intrusion by comparing an earmark to one previously provided. *Id.* at 979. Similarly, in another case, the Federal Circuit found claims to be directed to the abstract idea of "collecting and analyzing information to detect misuse and notifying a user when misuse is detected." *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1094 (Fed. Cir. 2016). There, the claims related to a system of detecting misuse by "analyzing data such as in log files," and recited several elements including generating a rule for monitoring audit log data, applying the rule, storing hits in memory, and providing notifications when hits occurred. *Id.* at 1093-94.

ii. The '489 Patent's Claims Lack an Inventive Concept

The claims of the '489 Patent additionally fail to recite an inventive concept, instead featuring a bare recitation of the abstract idea of detecting unauthorized users by baiting them with false information. The bare recitation of an idea "does nothing significant to differentiate a process from ordinary mental processes" excluded under 35 U.S.C. § 101. *Elec. Power Grp.,*, 830 F.3d at 1355. Where, as here, the asserted claims disclose "no more than an 'abstract idea garnished with accessories,'" courts will routinely dismiss claims as patent-ineligible at the pleading stage. *Ultramercial*, 772 F.3d at 719. Since the claims here "simply instruct the practitioner to implement the abstract idea . . . on a generic computer," they do not recite an inventive concept, and should be declared invalid. *Alice Corp.*, 573 U.S. at 225.

There are no allegations in Forescout's counterclaims that suggest anything inventive about the '489 Patent. Its entire set of allegations as to the content of the '489 Patent is as follows:

> *The '489 Patent discloses a method and a system for providing security to a network by at least identifying an unauthorized user who is attempting to gain access to a node on the network, and preferably by then actively blocking that unauthorized user from further activities. Detection is facilitated by the unauthorized user providing a "mark," or specially crafted false data, that the unauthorized user gathers during the information collection stage performed before an attack. The mark is designed such that any attempt by the unauthorized user to use such false data results in the immediate identification of the unauthorized user as hostile and indicates that an intrusion of the network is being attempted. Preferably, further access to the network is then blocked by diverting traffic from the unauthorized user to a secure zone, where the activities of the unauthorized user can be contained without damage to the network.*

Dkt. 107 ¶ 202. This brief paraphrasing of the first claim highlights details which "fall into one or both of two categories: they are themselves abstract; or there are no factual allegations from which one could plausibly infer that they are inventive." *SAP*, 898 F.3d at 1168-69. In such a circumstance, judgment on the pleadings is proper. *Id.* at 1169.

Further, no logical components or hardware (even conventional hardware) are expressly mentioned in Claim 1 of the '489 Patent or its dependents. Instead, the method consists of an unnamed actor "receiving" and "analyzing" communications to detect intrusion, and then "applying intrusion handling procedures" as needed. Arguably, the text of Claim 1 does not even explicitly exclude the *entire* method from being carried out by hand, with addressed letters being sent throughout a physical mail network. Regardless, to the extent the specification shows that the intent was for the method to be carried out on a computer network, it is clear that this would be a conventional network, and a method implemented on conventional hardware. '489 Patent at 3:60-4:25. This does not add "enough," as required by *Alice*, to transform the idea into an invention, and instead contemplates at most the use of "entirely conventional, generic technology" to implement the idea, and not the kind of "inventive distribution of functionality within a network" contemplated by courts. *Elec. Power Grp.*, 830 F.3d at 1355-56. To the extent the claims are limited to the field of securing computer networks, such language merely "attempts to limit the abstract concept to a computer implementation and to a specific industry," and will not create an inventive concept to allow patentability. *Accenture*, 728 F.3d at 1345. Indeed, the claims do not "purport to improve the functioning of the computer itself," as they are directed to an idea—basic deception—that could be carried out by hand, just applied to the field of computers. *Alice Corp.*, 573 U.S. at 225. Here, to the extent there is a "claimed configuration," it "does not add sufficient substance to the underlying abstract idea" and merely serves as "a conduit for the abstract idea," leaving the claim without an inventive concept. *Yu*, 1 F.4th, at 1045. This remains the case "even if [the claim] recites novel subject matter." *Id.* (citing *SAP*, 898 F.3d at 1163).

Forescout may argue that Claim 1's final step of "applying intrusion handling procedures" to the intruder's communications can suffice as an inventive concept. However, this step is nothing more than vaguely-defined extra-solution activity. As was the case in *Ultramercial*, the '489 Patent's claims do no more than "break the abstract idea into basic steps and add token extra-solution activity," which does not provide an inventive concept to convert the idea into patentable subject matter. 772 F.3d at 714. Indeed, even in *Ultramercial*, the "token extra-solution activity" included the specific requirement of "restricting public access" to content; here, post-solution activity is left vague, allowing the implementor to "apply" whatever generic "procedures" they see fit to communications once an intruder has been identified. *Id.* at 714-15.

The '489 Patent's claims recite the bare abstract idea of detecting unauthorized users by baiting them with false information. The text of the claims does not even expressly limit the idea to computer networks, and does not specify any configuration other than a presumed conventional computer network with conventional computers implementing the method of this abstract idea. In short, the claims are "recited at a high level of generality and merely invoke[] well-understood, routine, conventional components to apply [an] abstract idea." *Yu*, 1 F.4th at 1045.

b. U.S. Patent No. 10,652,116 (the '116 Patent)

The '116 Patent relates to device classification. In short, it claims the use of data from two sources to classify devices. It gathers this data by simply having the device provide it openly (*i.e.*, from a software agent on the device), or by monitoring its traffic. According to its specification, its claimed invention relates to the "classification of devices connected to a network" as "useful for monitoring and securing the communication network." '116 Patent at 1:14-16. It distinguishes itself from classification methodologies that "rely on [MAC] addresses and [HTTP] user-agent strings" which are "limited and narrow in their classification abilities" by instead being "based on information available via a communication network." *Id.* at 1:5-8, 18-24. To that end, it claims a method of detecting devices as they connect, accessing a "first data associated with the device" from an "agent" installed on the device, along with a "second data associated with the device" that is "traffic data," analyzing that data, determining a classification, and storing that classification. *Id.* at Claim 1. Its dependent claims add little, reciting, *e.g.*, "initiating an action based on the classification" (Claim 2), that the "traffic data" is "associated with a port of the device" (Claim 3) or "associated with a service of the device" (Claim 4), reciting types of "external systems" (Claim 5), reciting that data be received additionally from "another device communicatively coupled to the device" (Claim 6), reciting that the analysis be "passive traffic analysis," (Claim 7), or "active traffic analysis" (Claim 8), or that it be based on a "proximity" of the device to another device (Claim 9), or based on the "operating time" of the device (Claim 10), and system and medium claims.

Accordingly, the '116 Patent is directed to the abstract idea of classifying devices on a network. Its claims recite this bare idea, and do little more than "break the abstract idea into basic steps," with its implementation and structure left entirely open. *See Ultramercial*, 772 F.3d at 714. The first independent claim of the '116 Patent is representative, and recites:

> *1. A method comprising:*
>
> *detecting a device coupled to a network in response to the device being coupled to the network;*
>
> *accessing first data associated with the device from an agent installed on the device;*
>
> *accessing second data associated with the device from an external system, wherein the second data associated with the device comprises traffic data associated with the device;*
>
> *analyzing the traffic data of the device;*
>
> *determining a classification for the device based on the first data associated with device and the traffic data; and*
>
> *storing the classification for the device.*

'116 Patent, at Claim 1. As described below, this claim recites nothing more than an abstract idea, and an instruction to the reader to apply that idea in the context of a computer network, with the "token extra-solution activity" of storing the classification after it has been determined. Accordingly, the '116 Patent is invalid.

i. The '116 Patent's Claims are Directed to an Abstract Idea

The '116 Patent is directed to the abstract idea of classifying devices on a network. As the applicant explained during prosecution, the claims at the time were "directed to the classification of devices connect [sic] to a network based on the data associated with device [sic]." '116 File History, Response to Office Action of June 13, 2018 (Ex. A), at 7.[3] This is no less abstract than simply classifying devices on a network, as any classification is inherently based on data or information of

[3] The Applicant made this comment with respect to all of the claims pending at the time. While the broadest independent claim has since been narrowed and other claims have been amended, the character of the claims remains unchanged and the point still applies.

some kind. To be sure, the patent never asserts that there is anything unconventional about making a classification using data. Instead, the specification suggests that the entirety of the patent's supposed point of novelty is the use of *more* data, stating that "some" prior "classification methodologies rely on media access control (MAC) addresses and hypertext transfer protocol (HTTP) user-agent strings," which were error-prone. '116 Patent at 1:18-24; *see also* '116 File History, Response to Office Action of June 13, 2018 (Ex. A), at 7 (citing same). The claims, however, only describe the "data" being analyzed in extremely generic terms, referring to "data … from an agent," which could be any data about the device, and "traffic data" of the device. Arguably, the claims would even be satisfied by, *e.g.*, simply the collection of a MAC address—which is just a unique ID assigned to every network-capable machine—from an agent and/or traffic data, something the specification itself suggests. *See* '116 Patent, 4:19-37 ("agent 140 … configured to gather information … includ[ing] … MAC address …"); 6:26-28 ("[t]he traffic data may include … the media access control address (MAC address) …"). The Federal Circuit has found claims combining multiple sources of data to nonetheless be abstract. *See, e.g.*, *Credit Acceptance Corp. v. Westlake Servs.*, 859 F.3d 1044, 1054 (Fed. Cir. 2017) (finding claims reciting a method of "combining [] two sources of information to create a financing package" to be directed to an abstract idea); *Bozeman*, 955 F.3d at 979 (finding claims reciting a method of "reducing check fraud by receiving financial transaction data from two sources" to be directed to an abstract idea). Thus, these limitations are nothing more than token recitations as to data which fail to constrain the patent beyond a simple idea.

The abstract idea of classifying devices—dividing objects into categories—is a well-known method of organizing a human activity, whether done on a network or elsewhere. For example, librarians have long categorized books into classifications based on information about those books. As has been observed, the "concept of data collection, recognition, and storage is undisputedly well-known" and a task which "humans have always performed." *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat. Ass'n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014). Indeed, the Federal Circuit has found similar claims ineligible as directed to "the concept of classifying an image and storing the image based on its classification." *In re TLI Commc'ns, LLC Pat. Litig.*, 823 F.3d 607, 611 (Fed. Cir. 2016). In *TLI*, the claims included steps for recording images, storing images, transmitting data, receiving data, extracting classification information, and storing the images again. *Id.* at 610. While the court recognized that the claim included arguably "concrete, tangible components," these components were merely "a generic environment in which to carry out the abstract idea." *Id.* at 611. So too here, where the context of a network, and the recitation of the steps of "detecting a device coupled to a network" and "accessing data … from an external system" provide less than concrete structure, and more of a generic environment in which the classification of devices occurs.

The claims here are also not unlike those of *Yu*, which the Federal Circuit found to be directed to the abstract idea of taking two pictures and using one picture to enhance the other in some way. *Yu*, 1 F.4th at 1043. Like the '116 Patent's claims here, those claims recited the use of two forms of data to perform a simple task, enhancing an image, and in *Yu* even constrained the forms of data being used, noting that the two pictures may be at different exposures. *Id.* Just as the claims in *Yu* only recited "conventional camera components" to effectuate the idea, the claims here recite only conventional computer components—a generic "device," a generic "network," and a generic "external system." *Id.*; '116 Patent at Claim 1. The Federal Circuit has reached the same conclusion in a number of other cases with claims directed to similar abstract ideas. *See, e.g.*, *Bozeman*, 955 F.3d at 980 (finding data collection and analysis of data from physical documents to be "directed to the abstract idea of collecting and analyzing information for financial transaction fraud or error detection."); *Content Extraction*, 776 F.3d at 1347 (finding claims to be "drawn to the abstract idea of 1) collecting data, 2) recognizing certain data within the collected data set, and 3) storing that recognized data in a memory," noting that the "concept of data collection, recognition, and storage is undisputedly well-known"); *FairWarning IP*, 839 F.3d at 1094 (finding claims directed to "collecting and analyzing information to detect misuse and notifying a user when misuse is detected," despite claims reciting several elements including generating and applying rules, storing data in memory, and providing notifications). In all of these cases, some amount of "technical jargon" existed in the claims to provide a context which, upon closer inspection, provided no more than "a generic environment in which to carry out the abstract idea." *Ericsson*, 955 F.3d at 1326-27 (quoting *TLI Commc'ns*, 823 F.3d at 612). Accordingly, courts must look past any "technical jargon" to instead focus on the claim's "character as a whole," which—in the above-cited cases and in this case—is directed to a simple abstract idea. *Id.* (citing *Enfish*, 822 F.3d at 1335).

ii. The '116 Patent's Claims Lack an Inventive Concept

The claims of the '116 Patent additionally fail to recite an inventive concept, instead featuring a bare recitation of the abstract idea of classifying devices on a network, implemented using conventional computers in a network environment. That the classification involves certain broad types of generic data, that it occurs when a device connects to a network, and that it is then stored falls short of providing the type of inventive concept that "in practice amounts to significantly more than a patent upon the [ineligible concept] itself." *Alice*, 573 U.S. at 217-18 (alteration in original).

Forescout's counterclaims fail to suggest anything inventive about the '116 Patent, and instead merely "restate the abstract ideas" by summarizing the claims themselves. *PersonalWeb Techs.*, 2021 WL 3556889, at *6. Forescout's allegations as to the content of the '116 Patent is as follows:

> *The '116 Patent discloses systems, methods, and related technologies for device classification. In certain aspects, traffic data associated with a device and data from an external system can be accessed. The data can be processed to determine a device classification for the device. An action can be initiated according to the classification.*

Dkt. 107 ¶ 178. As in the claims themselves, there is nothing inventive alleged in Forescout's counterclaim, and with "no plausibly alleged innovation in the non-abstract application realm," judgment on the pleadings of invalidity is proper. *SAP*, 898 F.3d at 1163, 1169. In fact, Forescout's own description explains the abstract idea of the invention surprisingly well: data is "accessed," then "processed," and then an action "can" be initiated. Action needn't be taken to satisfy every claim, as Claim 1 specifies that merely "storing" the classification is enough, with Claim 2 adding the act of "initiating" an unspecified action based on the classification.

Further, only generically recited conventional hardware components are expressly mentioned in the claims of the '116 Patent. Claim 1 recites a "device," a "network," and an 'external system," all simple components that are "recited at a high level of generality" and used as mere "well-understood, routine, conventional components to apply [an] abstract idea." *Yu*, 1 F.4th at 1045. Moreover, the steps of "accessing" and "analyzing" data, along with "determining" a classification, are merely a recitation of the abstract idea itself. Nothing in the asserted claims adds "enough" to transform the idea into an invention, as the claims instead contemplate the use of "entirely conventional, generic technology" to implement the abstract idea. *Elec. Power Grp.*, 830 F.3d at 1353, 1356 (citation omitted). Nor does the "claimed configuration" provided by the inclusion of a basic network environment create an inventive concept, as it "does not add sufficient substance to the underlying abstract idea" and merely serves as "a conduit for the abstract idea." *Yu*, 1 F.4th at 1045 (citation omitted).

Finally, the steps in the method claim other than performing the classification itself are the sort of vaguely-defined extra-solution activity that the Federal Circuit has rejected as giving rise to an inventive concept under 35 U.S.C. § 101. *See Ultramercial*, 772 F.3d at 714. The claims provide, at most, a proposed time to classify devices (when they connect to the network), and proposed sources of data (data from an agent, and traffic data) to review when making that classification. Beyond this "token extra-solution activity," which mainly just provides a context for applying the abstract idea, the claims do no more than "break the abstract idea into basic steps," without the inventive concept needed to give rise to patentability. *Id.* at 714-15. Claim 2 adds the particularly vague step of "initiating an action based on the classification," which both highlights how abstract Claim 1 is, where no action need be taken, and provides no guidance as to what sort of action would be taken in response to such a classification, with no claims depending from Claim 2 to expand on this. Claims 11 and 15 both provide non-method claims which involve the act of carrying out a slightly reduced version of the abstract idea of Claim 1—based only a first data instead of two—and propose some "token extra-solution activity." Claim 11 directs the implementor to "apply a security policy" based on classification, and Claim 15 proposes that they "change network access" of the device based on its classification—not at all dissimilar from the "token" activity described in *Ultramercial*, which was to take the step of "restricting public access" to content. 772 F.3d at 715. In short, the claims are far from being those that "integrate the building blocks into something more," since in most of the claims, nothing is done with the classification once stored, and in the handful of claims that do invite the user to take the step of "initiating an action," that action is defined in a general, vague manner. *Alice*, 573 U.S. at 217 (citation omitted).

The '116 Patent's claims recite the abstract idea of classifying devices on a network, and lack any inventive concept sufficient to transform them into a patentable invention. The claims add little more to this idea than the environment in which the idea is being carried out, and, at most, the instruction to "apply it." *Alice*, 573 U.S. at 221. In short, the claims are "recited at a high level of generality and merely invoke[] well-understood, routine, conventional components to apply [an] abstract idea." *Yu*, 1 F.4th at 1045.

c. U.S. Patent No. 10,652,278 (the '278 Patent)

The '278 Patent relates to compliance monitoring. In short, it claims the act of checking if devices comply with a policy as they connect to a network, based on the type of device connecting. According to its specification, its claimed invention relates to "checking device compliance" and providing the "remediation of device compliance issues." '278 Patent at 1:5-8. Its claims are very similar in scope to those of the '116 Patent, with Claim 1 reciting detecting devices as they connect to the network, determining a classification of the device based on traffic information, accessing a standard-based compliance rule based on that classification, performing a compliance scan, determining a compliance level, and performing an action based on that compliance level. *Id.* at Claim 1. In other words, the '278 Patent claims classifying devices as they connect, and scanning them for standards-based compliance based on that classification. Its dependent claims add little, reciting, *e.g.*, a "compliance standard based compliance rule" (Claim 2), a "security content automation protocol" rule (Claim 3), the compliance rules being "associated with a security policy" (Claim 4), performing "another compliance scan" based on that "security policy" (Claim 5), taking action by "changing network access of the device" (Claim 6), performing the compliance scan "automatically" according to a security policy (Claim 7), associating the compliance rule with a value dubbed a "weight" (Claim 8), taking action by automatically initiating an "update service" (Claim 9), or initiating a "patch service" (Claim 10), the traffic information being one of an IP address, port, or protocol (Claim 11), and system and medium claims.

Thus, the '278 Patent is directed to the abstract idea of assessing compliance based on a device classification. Its claims recite this bare idea, a simple method of organizing a human activity applied to computers, and then instruct the implementor to merely "perform" an unstated "action" in response to its application of these generic rules. The first independent claim of the '278 Patent is representative, and recites:

> *1. A method comprising:*
>
> *detecting, by a compliance monitoring device, a device coupled to a network in response to the device being coupled to the network;*
>
> *determining a classification of the device based on traffic information associated with the device;*
>
> *accessing a compliance rule based on the classification of the device, wherein the compliance rule is a standard based compliance rule;*
>
> *performing, by a processing device of the compliance monitoring device, a compliance scan on the device based on the compliance rule;*
>
> *determining a compliance level of the device based on a result of the compliance scan of the device; and*
>
> *performing an action based on the compliance level.*

'278 Patent at Claim 1. As described below, this claim recites nothing more than an abstract idea, and an instruction to the reader to apply that idea in the context of a computer network, with the "token extra-solution activity" of "performing an action based on the compliance level." Accordingly, the '278 Patent is invalid.

i. The '278 Patent's Claims are Directed to an Abstract Idea

The '278 Patent is directed to the abstract idea of assessing compliance based on a device classification. This idea is similar to, and no less abstract than, the idea of the '116 Patent, discussed above, which was directed to classifying devices on a network. The idea of treating devices differently for compliance purposes is similarly a common method of organizing human activity. In human activity, classification is often a necessary step in assessing compliance with any set of regulations. For example, a building examiner would classify structures before inspecting them and applying building codes to them, as different classes of structures necessitate different regulations. Apart from the limited use of technical jargon and the automation of its implementation by a computer, the principle of the '278 Patent's claims is the same. Indeed, the claims reflect that, simply instructing the actor to classify devices before inspecting/scanning them and applying compliance rules to them, followed by the token step of "performing an action" based on that compliance level.

The Federal Circuit has considered a number of cases involving similar abstract ideas, including those discussed above with regard to the '116 Patent. As the Federal Circuit has observed, a "wide variety of well-known and other activities constitute abstract ideas." *Ericsson*, 955 F.3d at 1327 (citation omitted). For example, it has found similar claims to be directed to "the concept of classifying an image and storing the image based on its classification." *TLI Commc'ns*, 823 F.3d at 611. Much like *TLI*, the claims here boil down to performing a classification, and treating the classified items differently depending on their classes. While the claims here recite, for example, that a "compliance monitoring device" performs the detection of the devices as they connect to the network, '278 Patent at Claim 1, this is merely "a generic environment in which to carry out the abstract idea." *TLI Commc'ns*, 823 F.3d at 611. The compliance monitoring is described by the specification being as a device which "may be configured for a variety of tasks including performing compliance benchmarking or scanning of devices," and may be "a computing system" or a piece of generic exemplary conventional hardware. '278 Patent, at 4:12-30. In other words, the "compliance monitoring device" is a generic computer that does exactly what it sounds like it does: monitors for compliance. As the Federal Circuit has observed, when "the specification largely treats [a component] as a black box," and "discus[es] [the component] only in terms of non-limiting embodiments," as here, the component cannot "modify the focus of the claims" away from the abstract idea. *Dropbox, Inc. v. Synchronoss Techs., LLC*, 815 F. App'x 529, 533 (Fed. Cir. 2020).

ii. The '278 Patent's Claims Lack an Inventive Concept

The claims of the '278 Patent additionally fail to recite an inventive concept, instead featuring a bare recitation of the abstract idea of assessing compliance based on a device classification. The claims of the '278 Patent provide "no more than 'an abstract idea garnished with accessories,'"—a situation where courts will routinely dismiss claims at the pleading stage. *Ultramercial*, 772 F.3d at 719 (citation omitted). The fact that a "compliance monitoring device" is involved does not change this, as that device only performs two steps: detecting devices, and scanning those devices. It amounts to an instruction to simply apply the compliance scan as devices connect to the network, creating no more than "a generic environment in which to carry out the abstract idea." *Ericsson*, 955 F.3d at 1326-27 (citation omitted); *accord TLI Commc'ns*, 823 F.3d at 611.

Forescout's counterclaims again summarize the claims, rather than identifying anything inventive about the '278 Patent. This reinforces the idea that the claims merely "restate the abstract ideas." *Personalweb Techs.*, 2021 WL 3556889, at *6. Forescout's entire set of allegations as to the content of the '278 Patent is as follows:

> *The '278 Patent discloses systems, methods, and related technologies for device compliance monitoring. In certain aspects, one or more compliance rules associated with a device classification are used to determine a compliance level of a device. The one or more compliance rules may be based on a standard. An action can be initiated according to the compliance level.*

Dkt. 107 ¶ 207. The counterclaim, again, summarizes the abstract idea embodied in the claims: device compliance is monitored by applying rules associated with the classification of the device. If one were to replace the word "device" with "building" in Forescout's description of their patent, they would be left with a fair description of the human process of inspecting a building to see if it meets building standards:

> *In certain aspects, one or more compliance rules associated with a [building] classification are used to determine a compliance level of a [building]. The one or more compliance rules may be based on a standard. An action can be initiated according to the compliance level.*

This illustrates how the claims of the '278 Patent do little more than present an abstract idea in a "generic environment"—here, a computer network—that has otherwise been carried out by humans in other environments throughout history. *See Ericsson*, 955 F.3d at 1326-27; *TLI Commc'ns*, 823 F.3d at 611. Apart from this swap of environments, the idea is merely "garnished with accessories," *Ultramercial*, 772 F.3d at 719 (citation omitted), like a "compliance monitoring device" that, predictably, monitors compliance. '278 Patent at Claim 1.

Again, only generically recited conventional hardware components are mentioned in the claims of the '278 Patent. Claim 1 recites a "device," a "compliance monitoring device," and a "network." As discussed above with respect to step 1, these are simple components that are "recited at a high level of generality" and used as mere "well-understood, routine, conventional components to apply [an] abstract idea." *Yu*, 1 F.4th at 1045. The compliance monitoring device is recited as effectively a nonce for "means of monitoring compliance," when read with its description in the specification, and requires the application of no more than a generic computer. *See* '278 Patent, at 4:12-30. Moreover, the remaining steps of "detecting," a device, "determining" a classification, "accessing" a rule, and "determining" a compliance level are merely a restatement of the abstract idea itself, followed by an instruction to perform an action—any action—based on this determined level. Nothing in the asserted claims adds "enough," as required by *Alice*, to transform the idea into an invention, *see Alice Corp.*, 573 U.S. at 222-26, as the claims instead contemplate the use of "entirely conventional, generic technology" to implement the abstract idea, which is far from the kind of "arguably inventive distribution of functionality within a network" contemplated by courts. *Elec. Power Grp.*, 830 F.3d at 1355-56.

Moreover, to the extent the claims are limited to the field of securing computer networks, courts have found that "attempts to limit the abstract concept to a computer implementation and to a specific industry" will not create an inventive concept to allow patentability. *Accenture Glob.*, 728 F.3d at 1345. Indeed, the claims do not "purport to improve the functioning of the computer itself," *Alice Corp.*, 573 U.S. at 225, as they are directed to an idea—applying rules to devices based on classification—that could be carried out by hand, just applied to the field of computers. *See id.* at 225-26. The existence of a "compliance rule," specified more completely as an industry-standard type of rule called a "SCAP rule" in some dependent claims, does not change this. For example, in *FairWarning*, the Federal Circuit found claims that recited steps of, *inter alia*, generating a rule, applying it to log data, and finally storing and announcing results to merely be "directed to the broad concept of monitoring audit log data," far from the "technological advance relating to accessing and combining disparate information sources" the patentee claimed it to be. *FairWarning IP*, 839 F.3d at 1097. Further, the fact that these rules were applied to computer-specific log data did not create an inventive concept, as "limiting the claims to the computer field does not alone transform them into a patent-eligible application." *Id.*

Finally, the steps in the method claim other than performing the classification itself are the sort of vaguely-defined extra-solution activity that the Federal Circuit has rejected as giving rise to an inventive concept under 35 U.S.C. § 101. *See Ultramercial*, 772 F.3d at 714-15. The claims provide, at most, a proposed time to apply the compliance checks (when they connect to the network), and then propose that the actor engage in "performing an action" after the check. '278 Patent at Claim 1. Beyond this "token extra-solution activity," which mainly just provides a context for applying the abstract idea, the claims "do no more than break the abstract idea into basic steps," without the inventive concept needed to give rise to patentability. *Ultramercial*, 772 F.3d at 714-15. Only two claims provide a proposed action in response to a compliance level determination. Claims 9 and 10 propose the use of an "update service" or a "patch service" and amount to little more than the "token extra-solution activity" examined in *Ultramercial. See Ultramercial*, 772 F.3d at 714. They state, in entirely generic terms, that if something is found to be wrong with the device being examined, fix it by applying a generic "update" or "patch." How to apply an update or patch is left as an exercise to the reader, as the limitations really just recite, at most, an extension of the abstract idea: if something is wrong, fix it.

The '278 Patent's claims recite the abstract idea of assessing compliance based on a device classification, and lack any inventive concept sufficient to transform them into a patentable invention. The claims add little more to this idea than the environment in which the idea is being carried out, and, at most, the instruction to "apply it." As the Federal Circuit has observed, "limiting the claims to the computer field does not alone transform them into a patent-eligible application." *FairWarning IP*, 839 F.3d at 1097

d. U.S. Patent No. 10,530,764 (the '764 Patent)

The '764 Patent relates to post-connection client certificate authentication, with an emphasis on the post-connection timing. In short, it claims validating devices after they connect to a network by first quarantining them. According to its specification, it addresses problems with current authentication solutions that are "limited and narrow" and that "require precise configuration of many different network components." '764 Patent at 1:18-23. The specification asserts the claimed invention provides an "alternate to the pre-connect 802.1x protocol" in the form of a "post-connection client certificate authentication" method. '764 Patent at 2:21-25, 1:6-8 (emphasis added). Notably, while the claim recites the technical-sounding use and validation of digital certificates, this is not the focus of the invention—client certificates were used in the prior art protocol (802.1x) already. '764 Patent at 2:6-9. Instead, the patent and the claims focus on timing of this activity during the post-connection period as supposedly innovative. Claim 1 recites specifically a system which detects an endpoint device as it connects, restricts access of the device through typical means (a VLAN assignment), connects to it, and validates its client certificate in the usual way (by receiving it, a certificate from the authority validating it, and verifying the signatures and subject name of the devices), before granting the device further access. '764 Patent at Claim 1. In other words, it claims quarantining devices as the connect to the network until they present a valid certificate. The dependent claims add little more, reciting, *e.g.*, receiving a communication request from an agent on the endpoint device (Claim 2), monitoring traffic through the switch to detect the device's presence (Claim 3), updating access control lists to grant access after validation (Claim 4), and not restricting access if a network access control device suffers a failure during authentication (Claim 5), along with method and medium claims.

The '764 Patent is directed to the abstract idea of validating authorization after connection. It recites this bare idea, implemented using conventional computer technology components in the usual way. Though "written in technical jargon," *Ericsson*, 955 F.3d at 1326, it describes the conventional act of validating a digital certificate presented by software running on client devices on a network, the digital equivalent of a common method of organizing human activity, checking ID. *See id.* The first independent claim of the '764 Patent is representative, and recites:

> *1. A system comprising:*
>
> *a memory; and*
>
> *a processing device operatively coupled to the memory, the processing device to:*
>
> > *detect a connection of an endpoint device at a network switch coupled to a network;*
> >
> > *restrict access of the endpoint device to prevent the endpoint device from accessing resources of the network by applying a VLAN assignment to the network switch;*
> >
> > *establish a connection with the endpoint device;*
> >
> > *validate a client certificate corresponding to the endpoint device to authenticate the endpoint device as a corporate device, wherein to validate the client certificate, the processing device to:*
> >
> > > *receive the client certificate from the endpoint device, the client certificate comprising a subject name, a client public key and a digital signature of the client public key by a certificate authority;*
> > >
> > > *retrieve a certificate authority certificate from the certificate authority, the certificate authority certificate comprising a certificate public key;*

> *verify the digital signature of the client public key using the certificate authority public key; and*
>
> *verify the subject name using the client public key; and*
>
> *grant the endpoint device access to the resources of the network.*

'764 Patent at Claim 1. As described below, this claim recites nothing more than an abstract idea, a method of organizing human activity, that is implemented using generic computer hardware components to perform their conventional functions in their conventional arrangement. Accordingly, the '764 Patent is invalid.

i. The '764 Patent's Claims are Directed to an Abstract Idea

The '764 Patent is directed to the abstract idea of validating authorization after connection. The claims are "written in technical jargon," *Ericsson*, 955 F.3d at 1326, explaining the conventional process of validating a client certificate in four steps, despite the fact that this is the usual way of validating a client certificate. *See id.* at 1326-27. The claims, then, really boil down to the difference between checking ID at the door, and checking ID in the lobby. The specification takes pains to remind the reader of what it *hasn't* invented, distinguishing its claimed invention from the known "802.1x protocol which ensures connecting devices are authenticated using an X.509 digital certificate, or other credentials, prior to even gaining access to the network." '764 Patent at 2:6-9. This prior art is, then, the well-known method of checking ID at the door. The change in the '764 Patent comes from "using a post-connect paradigm." *Id.* at 2:23-24. This is the so-called inventive, but ultimately abstract, idea of checking ID at the lobby. Every element of the claim is merely part of a restatement of this idea, implemented with generic computer components performing their usual functions: detecting a user connecting to the network (or, in a hypothetical human activity, as they approach a checkpoint in the lobby), restricting their access (stop them at the desk), establishing a connection with them (asking them for their corporate ID), validating their certificate to validate the device as a corporate device (validating their corporate ID) by receiving it (having them hand it to someone at the desk), checking the certificate authority's signature (making sure it, *e.g.*, bears the seal of a corporation that issued it), verifying the subject name (verifying their name and photo), and then granting them access (letting them in). In short, the so-called improvement of this patent is an abstract one, implemented, effectively by its own admission, "using conventional and well-understood techniques." *Dropbox*, 815 F. App'x at 536.

The claims invalidated in *Ericsson* contained many similar elements of "technical jargon," *Ericsson*, 955 F.3d at 1326, but nonetheless were found to recite the abstract idea of "controlling access to, or limiting permission to, resources." *Id.* The patent at issue in *Ericsson* recited a "platform" having a "services component" and an "interface component," along with an "access controller," an "interception module," a "decision entity," and other components, arranged in a way that was purportedly unconventional. *Id.* at 1325-26. Given the breadth of the claims, however, these components were found to "collapse into" the abstract idea, as several logical components could be implemented by the same actual component. *Id.* at 1326. So too here, though the patent claims a "system," this system is a single generic computer which carries out the entire method. Much like the claims in *Ericsson* that were found to "collapse into" a single machine that received an access request and determined if that request should be granted, surrounded by boilerplate, *id.*, the claims here are already drafted that way. Similarly, the claims here do not recite how to "validate" a certificate, other than to individually validate its constituent components, which really just "collapses into" the abstract step of validating the certificate. *See id.* Just as the claims in *Ericsson* left the actor to "determine" if an access request should be granted by generic means, the claims here leave the system to "validate" a certificate by generic, conventional means.

ii. The '764 Patent's Claims Lack an Inventive Concept

The claims of the '764 Patent additionally fail to recite an inventive concept, instead featuring a bare recitation of the abstract idea of validating authorization after connection, implemented using conventional computers and conventional software, placed into a generic network environment. Such claims should be invalidated at the pleading stage as they provide "no more than 'an abstract idea garnished with accessories,'" *Ultramercial*, 772 F.3d at 719 (citation omitted), and nothing recited in the claims "in practice amounts to significantly more than a patent upon the [ineligible concept] itself." *Alice Corp.*, 573 U.S. at 217-18 (alteration in original) (citation omitted).

Forescout's counterclaims suggest nothing inventive about the '764 Patent, instead summarizing the abstract idea of the claims and the generic network environment in which the idea is carried out. Forescout's allegations as to the content of the '764 Patent are as follows:

> *The '764 Patent discloses a NAC device that detects a connection of an endpoint device at a network switch coupled to a network and restricts access of the endpoint device to prevent the endpoint device from accessing resources of the network. The NAC device establishes a connection with the endpoint device, validates a client certificate corresponding to the endpoint device to authenticate the endpoint device as a corporate device, and grants the endpoint device access to the resources of the network.*

Dkt. 107 ¶ 186. This paragraph describes the disclosure as referring to a "NAC device" that carries out the claims, although the claims themselves are broader than this. Further, the description emphasizes that an endpoint device is coupled to a network switch—but this is a conventional arrangement, and in any event provides no more than "a particular environment" (here, a conventional network) in which to carry out the invention. *Ericsson*, 955 F.3d at 1327 (citation omitted). It then restates the abstract idea: the device quarantines the endpoint, connects to the endpoint, validates its corporate certificate, and grants it access to the network. The claims recite this idea in "technical jargon," as in *Ericsson* (*id.* at 1326), and do "no more than break the abstract idea into basic steps" in this jargon. *Ultramercial*, 772 F.3d at 714-15. They recite substeps for two of these steps, which effectively reiterate the steps in more technical language: the claims recite steps of validating a certificate (by validating its constituent parts, much the same as the method for eating an elephant: one bite at a time), and recite using a VLAN assignment on the network switch to restrict access to the endpoint (which is technical jargon for asking the switch to quarantine the device to a "virtual" network, *see* '764 Patent at 4:59-61).

Moreover, to the extent the claims are limited to the field of securing computer networks, courts have found that "attempts to limit the abstract concept to a computer implementation and to a specific industry" will not create an inventive concept to allow patentability. *Accenture Glob.*, 728 F.3d at 1345. Indeed, the claims do not "purport to improve the functioning of the computer itself," *Alice Corp.*, 573 U.S. at 225, as they are directed to an idea—validating authentication after connection —that could be carried out by hand, just applied to the field of computers. *See id.* at 225-26. Here, the limited "claimed configuration" is one that is admittedly far from novel, as the specification itself notes that the conventional and well-known 802.1x industry standard differs from the claimed invention primarily in *when* the authentication takes place. In other words, the supposed improvement of the '764 Patent is an abstract one. It is one that "does not add sufficient substance to the underlying abstract idea" and merely serves as "a conduit for the abstract idea," resulting in a claim that is missing an inventive concept. *Yu*, 1 F.4th at 1045 (citation omitted).

Finally, the steps in the method claim other than performing the authorization itself are the sort of vaguely-defined extra-solution activity that the Federal Circuit has rejected as giving rise to an inventive concept under 35 U.S.C. § 101. *See Ultramercial*, 772 F.3d at 714. Just like the step of "restricting public access" to content was "token" activity in *Ultramercial*, *see id.* at 714-16, the activity surrounding the abstract idea in the claims of the '764 Patent is merely restricting access to the network by quarantining the device. In other words, the claims are far from being claims that "integrate the building blocks into something more," *Alice Corp.*, 573 U.S. at 217, since, apart from the technical recitation of the abstract idea, there is nothing more in the claims.

The '764 Patent's claims recite the abstract idea of classifying devices on a network, and lack any inventive concept sufficient to transform them into a patentable invention. The claims add little more to this idea than the environment in which the idea is being carried out, and, at most, the instruction to "apply it." In short, the claims are "recited at a high level of generality and merely invoke[] well-understood, routine, conventional components to apply [an] abstract idea." *Yu*, 1 F.4th at 1045.

2. Forescout's Claim for Tortious Interference Should Be Dismissed

Fortinet filed its Complaint on May 15, 2020 (Dkt. No. 1) asserting three patents, and its Amended Complaint on December 2, 2020 (Docket No. 67) further asserting an additional two patents. Forescout moved to dismiss these complaints twice for failure to state a claim on the grounds that (1) Fortinet's patents claim ineligible subject matter and (2) Fortinet failed adequately to plead indirect infringement or willful infringement. Dkt. Nos. 24 and 71. After two rounds of briefing, the Court maintained Fortinet's indirect infringement allegations and declined to find Fortinet's patents invalid, but dismissed Fortinet's willful infringement allegations as not rising to the level of "'egregious infringement behavior' that the Supreme Court has identified as meriting enhanced damages for infringement." Dkt. 94 at 34 (citation omitted); *see also* Dkt. No. 55.

Following the filing of the initial Complaint, Forescout alleges that Fortinet made two types of communications to the press and to customers regarding Forescout. First, Forescout alleges that Fortinet "republished" its patent infringement complaint allegations to the media ("republishing allegations"). Ans. ¶ 142. Second, and separately, Forescout alleges that Fortinet made statements regarding Forescout's dealings with Advent International ("Advent"). In May, 2020, Advent decided not to proceed with a planned acquisition of Forescout. Ans. ¶ 144. Forescout alleges that Fortinet then "told Forescout's existing and potential customers that Forescout's financial solvency was in doubt" by allegedly telling customers that "[Forescout's] acquisition by Advent and bid to be taken private was put on hold resulting in Forescout now filing a lawsuit against Advent, all this leaving Forescout on uncertain ground financially" ("financial allegations"). Ans. ¶ 145.

Forescout's Claim I for tortious interference with business relationships must fail for at least three reasons. First, the Federal Circuit has confirmed that tortious interference claims for communications related to patent infringement claims are preempted under federal law with very limited exceptions. Forescout's Claim I does not fall within one of those exceptions and accordingly, at least Forescout's republishing claims are preempted as a matter of law. Second, Forescout's financial allegations must be dismissed as outside of this Court's subject matter jurisdiction as a state law claim not related to any claim over which the Court has independent jurisdiction. Third, at least Forescout's allegations must also be dismissed for failing to state a claim upon which relief may be granted as Forescout has not alleged facts (1) giving rise to an independently actionable wrongful act or (2) identifying a specific business relation that was interfered with as a result of Fortinet's alleged statements.

a. The "Republishing" Tortious Interference Allegations are Preempted by Federal Law

Forescout alleges that Fortinet tortiously interfered with its business relationships by "republishing" its patent infringement allegations against Forescout to Forescout's current or potential customers, either by direct communication or through publicity. *See* Ans. at ¶¶ 142, 145. However, Fortinet is absolutely entitled to communicate with third parties about its patent rights and its publicly-filed allegations. Such conduct cannot be the basis of a tortious interference claim, as these acts are protected under federal law, which preempts Forescout's state law tort claims based on such communications.

It is well established that "federal patent laws . . . bar state-law liability for communications concerning alleged infringement so long as those communications are not made in 'bad faith.'" *Globetrotter Software, Inc. v. Elan Comput. Grp., Inc.*, 362 F.3d 1367, 1374-75 (Fed. Cir. 2004); *id.* at 1374 ("State-law claims . . . can survive federal preemption only to the extent that those claims are based on a showing of 'bad faith' action in asserting infringement." (citation omitted)). As explained above, such preemption extends to communications made to the marketplace, as "federal patent law bars the imposition of liability for publicizing a patent in the marketplace unless the plaintiff can show that the patentholder acted in bad faith." *Hunter Douglas, Inc. v. Harmonic Design, Inc.*, 153 F.3d 1318, 1336 (Fed. Cir. 1998), *overruled on other grounds en banc by Midwest Indus., Inc. v. Karavan Trailers, Inc.*, 175 F.3d 1356 (Fed. Cir. 1999). Indeed, a "[p]laintiff is entitled to communicate facts about its suit in the marketplace, including accusations of infringement, consistent with its allegations in suit." *Wilco AG v. Packaging Techs. & Inspection LLC*, 615 F. Supp. 2d 320, 325 (D. Del. 2009). The Federal Circuit "has uniformly upheld a patentee's right to publicize the issuance of patents and to so inform potential infringers," and further confirmed that "a competitive commercial purpose is not of itself improper." *Mikohn Gaming Corp. v. Acres Gaming, Inc.*, 165 F.3d 891, 897 (Fed. Cir. 1998). Notably, Forescout's customers are identified as direct infringers in Fortinet's Complaints. Dkt. 67 ¶¶ 3, 46-49, 61-64, 76-79, 91-94, 106-109.

The "bad faith" requirement to avoid preemption has two components: first, "[t]he objective component requires a showing that the infringement allegations are 'objectively baseless,'" *i.e.*, that "no reasonable litigant could realistically expect success on the merits"; second, "[t]he subjective component relates to a showing that the patentee in enforcing the patent demonstrated subjective bad faith." *800 Adept, Inc. v. Murex Sec., Ltd.*, 539 F.3d 1354, 1370 (Fed. Cir. 2008) (citations omitted). Both elements must be shown in order to support a finding of bad faith, as "an objectively reasonable effort to litigate cannot be [a] sham regardless of subjective intent." *Globetrotter Software*, 362 F.3d at 1375-76 (quoting *Prof'l Real Estate Invs., Inc. v. Columbia Pictures Indus., Inc.*, 508 U.S. 49, 57 (1993)). An action where the claimant purports to "show [bad faith] only through attempts to demonstrate subjective bad faith" must therefore fail. *Id.* at 1375; *see also GP Indus., Inc. v. Eran Indus., Inc.*, 500 F.3d 1369, 1375 (Fed. Cir. 2007) (in evaluating bad faith, a court applies the wrong standard by focusing on subjective intent, as "[s]ubjective considerations of bad faith are irrelevant if the [infringement] assertions are not objectively baseless"). To avoid preemption at the motion to dismiss phase, "bald assertions that [the patent owner] acted in 'bad faith'" are insufficient. *Matthews Int'l Corp. v. Biosafe Eng'g, LLC*, 695 F.3d 1322, 1332 n.5 (Fed. Cir. 2012); *see id.* at 1332-33 (affirming dismissal of state law claims because of preemption). Instead, in evaluating the objective prong, the Federal Circuit has held that a court must examine "convincing objective factors" as to the objective baselessness of the lawsuit. *GP Indus.*, 500 F.3d at 1375.

Forescout's tort counterclaim fails to state a claim with regard to its republishing allegations because Forescout cannot satisfy at least the first, objective prong of the *Globetrotter* test.[4] Forescout has failed to allege any facts—or, "convincing objective factors," *GP Industries*, 500 F.3d at 1375—establishing that Fortinet's lawsuit is objectively baseless such that "no reasonable litigant could realistically expect success on the merits." *Globetrotter Software*, 362 F.3d at 1376 (citation omitted). The standard for objective baselessness is not easily met, as "sham litigation must constitute the pursuit of claims so baseless that no reasonable litigant could realistically expect to secure favorable relief." *Prof'l Real Estate Invs., Inc. v. Columbia Pictures Indus., Inc.*, 508 U.S. 49, 62 (1993); *see also Dominant Semiconductors Sdn. Bhd. v. OSRAM GmbH*, 524 F.3d 1254, 1260 (Fed. Cir. 2008) ("To be objectively baseless, the infringement allegations must be such that 'no reasonable litigant could reasonably expect success on the merits.'" (citations omitted)).

[4] Forescout also cannot satisfy the subjective prong, including because Forescout's allegations about Fortinet's intent are at best misleading. While telling this Court that the Fortinet's lawsuit disrupted the Advent acquisition, Forescout previously told another court a very different story: "Lest the Court have any doubt about Advent's motivations in trying to walk away from the deal, just days before the merger was set to close, Advent's representative admitted to Forescout's CEO that its new distaste for the merger was all 'COVID-related.'" Verified Complaint ¶ 1, *Forescout Techs., Inc. v. Ferrari Grp. Holding L.P.*, No. 2020-0385 (Del. Ch. filed May 19, 2020) (Ex. C). However, since courts most often dismiss tortious interference claims as preempted after solely evaluating the objective prong, Fortinet has focused its briefing on that prong.

Here, Forescout offers only conclusory allegations as to non-infringement and invalidity, ignoring (1) that Fortinet's patents are entitled to a presumption of validity, and (2) that Fortinet's lawsuit has already survived multiple motions to dismiss. Specifically, Forescout alleges that Fortinet "knew, or should have known, [the asserted patents] were invalid and/or not infringed by Forescout." Ans. ¶¶ 141, 147. These are run-of-the-mill defenses to patent infringement and insufficient to allege that Fortinet's lawsuit is objectively baseless.[5] *See Globe Cotyarn Pvt. Ltd. v. Next Creations Holdings LLC*, No. 18 Civ. 04208 (ER), 2020 WL 4586892, at *6-7 (S.D.N.Y. Aug. 10, 2020) (refusing to find claims objectively baseless even where prior art presented at a previous International Trade Commission hearing indicated that at least portions of the asserted patents were invalid). Without facts alleged that would show that Fortinet's lawsuit is objectively unreasonable, Forescout's claim regarding patent-related communications must be dismissed. *See Mikohn Gaming*, 165 F.3d at 893-94, 896-97 (instructing, in a case where a patentee issued a press release and sent letters to actual and potential customers of the accused infringer, that "[i]n general, a threshold showing of incorrectness or falsity, or disregard for either, is required in order to find bad faith in the communication of information about the existence or pendency of patent rights").[6]

On facts such as these, courts regularly dismiss claims for tortious interference as preempted. For example, in *SanDisk Corp. v. LSI Corp.*, No. C 09-02737 WHA, 2009 WL 3047375 (N.D. Cal. Sept. 18, 2009), Judge Alsup found that a defendant had "failed to support its [interference] allegations with facts that [would] allow the Court to reasonably infer that defendant acted in bad faith," *id.* at *2, and dismissed the claim as preempted. *Id.* at *3. Though SanDisk alleged that "LSI sent letters to SanDisk's customers containing information that LSI 'knew or should have known was false,'" the *SanDisk* Court instructed that "[c]onclusory statements, however, are not sufficient to meet the pleading requirements," and found that "SanDisk is merely stating what it believes without

[5] It is Forescout, and not Fortinet, "who has the burden . . . to provide caselaw supporting the contention that [Fortinet's] claim of infringement was objectively baseless." *SanDisk*, 2009 WL 3047375, at *2 n. 4.

[6] Moreover, Fortinet has provided over 700 pages of detailed infringement contentions, reasonably disputes Forescout's claims of invalidity, and—of particular note—Fortinet's complaints have survived two motions to dismiss on the pleadings, and Fortinet's patents have all survived motions to dismiss under 35 U.S.C. § 101. Dkt. 55, 92, 94. Though Forescout alleges that the Court has "expressed skepticism about the validity" of the patents, Dkt. 107 ¶ 147, the Court did not invalidate them. Dkt. 55, 92, 94. Per the Federal Circuit, a "close question" establishes that infringement "assertions were not objectively baseless." *GP Indus.*, 500 F.3d at 1735.

providing any specific facts showing the basis for its information and beliefs. Such statements, which are not amplified by any facts, do not allow a judge to make any reasonable inferences of bad faith." *Id.* at *2 (citation omitted). Moreover, the court found that "SanDisk's allegations [did] not establish that LSI's claim of infringement was objectively baseless" because, in making its infringement claims, LSI had "analyzed plaintiff's products, determined that plaintiff's products infringe, and provided specific patents that [were] allegedly infringed." *Id.* The *SanDisk* court held that such analysis—which Fortinet has presented many times over in its Complaints, motion to dismiss briefing, and infringement contentions—"show[ed] that LSI was not just making conclusory statements" of infringement. *Id.* On that basis, the court found that "SanDisk has failed to [meet] its burden of proving that LSI's claim of infringement was objectively baseless," and held that its "state law claims are preempted by federal patent law because SanDisk has failed to sufficiently plead a case showing that LSI acted in bad faith." *Id.* at *2-3.

A similar result was reached in *Armstrong World Industries, Inc. v. Congoleum Corp.*, No. 09-3618, 2009 WL 10739028 (E.D. Pa. Dec. 29, 2009), where a tortious interference claimant's allegation that the patentee "knows or should know that its patent is not infringed, invalid and/or unenforceable" was found "insufficient to plead bad faith and sustain a state law claim of tortious interference." *Id.* at *2-3. Accordingly, the motion to dismiss was granted as "Armstrong ha[d] not sufficiently pleaded Congoleum's [b]ad faith in publicizing its patent, thereby causing the state law tortious interference claim to be preempted by federal patent law." *Id.* at *3. Likewise, in *Phishme, Inc. v. Wombat Security Technologies, Inc.*, No. 16-403-LPS-CJB, 2017 WL 3821107 (D. Del. Aug. 31, 2017), the court found a tortious interference claim preempted for lack of bad faith on facts rather similar to those of the present case: following a complaint for infringement of its patent, a plaintiff issued a press release that stated that the suit was a result of defendant's infringement and that plaintiff has "clear evidence" of the infringement, and further "sent similar emails to other existing and prospective customers of [defendant]." *Id.* at *4 (citations omitted). The defendant identified multiple types of harm, including customers electing not to contract with defendant, as well as derailing defendant's efforts to fundraise from third parties by effectively lowering defendant's valuation. *Id.* Though the defendant included a detailed explanation in its counterclaim explaining its view as to why plaintiff's then-discarded infringement allegation was baseless, *id.* at *5-6, the court found that the defendant "has not sufficiently pleaded objective bad faith, as required in order to overcome Patent Act preemption of [a] tortious interference state law counterclaim," *id.* at *5—and, even if defendant's position were eventually to prevail, defendant "still would not have demonstrated that it is plausible that [plaintiff] had an objectively baseless infringement claim." *Id.* at *7.

Accordingly, because Forescout has failed to properly plead that Fortinet's infringement lawsuit is objectively unreasonable, any tortious interference claim based on republishing allegations is preempted and should be dismissed. *See Matthews Int'l Corp.*, 695 F.3d at 1332-33 ("Because [claimant] points to nothing to indicate that [patentee's] alleged infringement allegations were so unreasonable as to be objectively baseless, the trial court correctly concluded that Matthews failed to sufficiently plead the bad faith element necessary to support its state-law claims.").

b. There is No Subject Matter Jurisdiction for Forescout's Remaining Tortious Interference Claim

As Forescout concedes, the only basis for the Court to have subject matter jurisdiction over Count I is through supplemental jurisdiction pursuant to 28 U.S.C. § 1367. Ans. ¶ 129. However, supplemental jurisdiction is not available here, at least with regard to Forescout's Advent-related financial allegations. In order for Forescout's tortious interference claim to fall within the Court's supplemental jurisdiction, it must be "so related" to Fortinet's patent claims that "they form part of the same case or controversy." 28 U.S.C. § 1367(a). "A state law claim is part of the same case or controversy when it shares a 'common nucleus of operative fact' with the federal claims . . . ." *Eastman v. Apple Inc.*, No. 18-cv-05929-JST, 2018 WL 5982440, at *3 (N.D. Cal. Nov. 14, 2018) (citations omitted). However, simply sharing a factual background is insufficient to establish a "common nucleus of operative fact." *Microthin.com, Inc. v. Silinconezone USA, LLC,* No. 06 C 1522, 2006 WL 3302825, at *3 (N.D. Ill. Nov. 14, 2006). Rather, "courts look to whether the state claims can be resolved or dismissed without affecting the federal claims." *Id.*

Thus, for those of Forescout's tortious interference allegations that are distinct enough from the patent-related republishing allegations and thereby avoid preemption, there is no subject matter jurisdiction over such claims. The allegations related to Forescout's financial situation—that Fortinet told customers that Advent's acquisition was on hold "leaving Forescout on uncertain ground financially (Ans. ¶ 145)—bear no relation to even the *subject matter* of the case or controversy regarding Fortinet's patent infringement allegations. The two certainly do not arise out of the same nucleus of operative fact, as even the internal communication describing Forescout's financial issues (see Ans. ¶ 145) is separate from the public statement Fortinet made regarding the substance of the litigation (see Ans. ¶ 142). Accordingly, this Court has no subject matter jurisdiction over any such claim.

In fact, Fortinet submits that the entirety of Forescout's tortious interference claim may lack subject matter jurisdiction. With regard to even the republishing allegations, resolution of Forescout's tortious interference claim will have no effect on the resolution of the patent infringement claims. As the court held in *Microthin.com, Inc.*, the operative facts required to prove patent infringement are not sufficiently related to the facts required to prove tortious interference with a business relationship, even when the allegedly tortious activity transpired as a result of the patent dispute. *Id.* at *4. Here, the operative facts alleged in support of Forescout's claim of tortious interference, including that certain statements were made to customers, Fortinet's intent, and the supposed effect these actions had on Forescout's business (Ans. ¶¶ 149-153), have no relation to whether the patents at issue were actually infringed. *Microthin.com, Inc.*, 2018 WL 5982440, at *4. Furthermore, the mere fact that the tortious interference claims arose as a result of the patent dispute is not enough to support the extension of supplemental jurisdiction over Forescout's state law claim. *Id.*

c. Forescout Also Fails to State a Plausible Claim

Putting aside the federal law preempted portions of Forescout's Count I, Forescout has failed to adequately plead two elements of its tortious interference claims. It has not pled that Fortinet committed an independently actionable wrong, and it has not identified a specific business relationship with which Fortinet allegedly interfered.

Under California law, tortious interference is not "a wrong in and of itself," and instead a plaintiff must allege facts showing "that the defendant engaged in an independently wrongful act."

Korea Supply Co. v. Lockheed Martin Corp., 29 Cal. 4th 1134, 1158 (2003). Improper motive is not enough, however, as the act must be "proscribed by some constitutional, statutory, regulatory, common law, or other determinable legal standard." *Id.* at 1159; *see also Prostar Wireless Grp., LLC v. Domino's Pizza, Inc.*, 360 F. Supp. 3d 994, 1016 (N.D. Cal. 2018).

Forescout's counterclaims focus almost entirely on Fortinet's alleged wrongful motive. Dkt. 107 ¶¶ 149-150. But as for the underlying act, Fortinet's allegations are sparse. As explained above, Forescout has not properly plead that Forescout's assertion of its patents against Forescout was objectively baseless. Forescout has additionally alleged that Fortinet informed Forescout's "existing and potential customers" that Forescout's Advent acquisition was "on hold" which resulted in leaving it "on uncertain ground financially." *Id.* ¶ 145. Forescout extrapolates from this act its own interpretation that Fortinet "falsely told" customers that "Forescout's financial solvency was in doubt." *Id.* Forescout has not, however, alleged that Fortinet's actual alleged statements constitute an independently wrongful act, such as libel[7] or trade libel—and indeed, they do not.

First, the alleged statements constitute opinions as to Forescout's financial position, not statements of fact, and thus are protected against any libel claim under the First Amendment. To plead libel, "the dispositive question is whether a reasonable fact finder could conclude the published statement declares or implies a provably false assertion of fact." *Integrated Healthcare Holdings, Inc. v. Fitzgibbons*, 140 Cal. App. 4th 515, 527 (2006). In *Integrated Healthcare*, the California Court of Appeal, Fourth District, examined statements similar to Forescout's allegations. There, the defendant stated that the plaintiff "appears to be underwater" with respect to its financial situation, based upon stated facts about its liabilities and rate of hospital admissions. *Id.* Because the underlying facts were true, the court held that the opinions based upon those stated facts were protected. *Id.* Here, Fortinet's alleged statement is based upon the stated fact that the Advent merger was on hold, a fact which is true, as even Forescout has admitted. *See* Dkt. 107 ¶ 144. For that reason, Fortinet's alleged statement

[7] Even if it were actionable, were Forescout to attempt to bring an independent libel action, it would be barred by the one year statute of limitations in California, as Forescout has alleged the statements were made in May and June of 2020, more than one year prior to the filing of its claims in July of 2021. *See* Cal. Civ. Proc. Code § 340(c).

is protected, and cannot constitute libel, or support a claim for tortious interference, under California law.

Second, Forescout fails to "identify particular customers and transactions of which it was deprived as a result of the libel," and thus fails to plead a claim for trade libel. *Piping Rock Partners, Inc. v. David Lerner Assocs., Inc.*, 946 F. Supp. 2d 957, 981 (N.D. Cal. 2013), *aff'd*, 609 F. App'x 497 (9th Cir. 2015) (emphasis added). For this same reason, Forescout also fails to plead an element of its tortious interference claim. California law requires that Forescout provide "evidence of specific economic relationships that were disrupted" by the alleged conduct, which is a far cry from Forescout's general allegations that Fortinet interfered with its "existing and prospective customers." *Rickards v. Canine Eye Registration Found., Inc.*, 704 F.2d 1449, 1456 (9th Cir. 1983); Dkt. 107 ¶ 149. As courts in this district have held, the party asserting tortious interference "must identify in some manner an economic relationship with a specific individual" to adequately plead its claim. *RingCentral, Inc. v. Nextiva, Inc.*, No. 19-CV-02626-NC, 2020 WL 4039322, at *5 (N.D. Cal. July 17, 2020) (emphasis added); *see also, e.g.*, *Google Inc. v. American Blind & Wallpaper Factory, Inc.*, 2005 WL 832398, at *8 (N.D. Cal. Mar. 30, 2005) (relationship with "repeat customers" was too speculative and did not "rise to the level of the requisite promise of future economic advantage"). Here, Forescout has not done so, alleging only that its relationship with its "existing and potential customers" was impacted, without identifying any specific business relationships (Dkt. 107 ¶ 149)—and thus its claim must fail.

IV. CONCLUSION

For the reasons stated above, Fortinet requests that the Court dismiss Counts I, VIII, IX, XI, and XII of Forescout's Counterclaims with prejudice pursuant to Rule 12(b)(6).

DATED: August 17, 2021

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

By: *[/s/ John M. Neukom]*
JOHN M. NEUKOM
Attorney for Plaintiff
FORTINET, INC.